

RICHARD E. NEAL,
MASSACHUSETTS,
CHAIRMAN

Congress of the United States

U.S. House of Representatives

COMMITTEE ON WAYS AND MEANS

1102 LONGWORTH HOUSE OFFICE BUILDING
(202) 225-3625

Washington, DC 20515-0348

<http://waysandmeans.house.gov>

KEVIN BRADY,
TEXAS,
RANKING MEMBER

JOHN LEWIS, GEORGIA
LLOYD DOGGETT, TEXAS
MIKE THOMPSON, CALIFORNIA
JOHN B. LARSON, CONNECTICUT
EARL BLUMENAUER, OREGON
RON KIND, WISCONSIN
BILL PASCRELL JR., NEW JERSEY
DANNY K. DAVIS, ILLINOIS
LINDA T. SANCHEZ, CALIFORNIA
BRIAN HIGGINS, NEW YORK
TERRI A. SEWELL, ALABAMA
SUZAN DELBENE, WASHINGTON
JUDY CHU, CALIFORNIA
GWEN MOORE, WISCONSIN
DAN KILDEE, MICHIGAN
BRENDAN BOYLE, PENNSYLVANIA
DON BEYER, VIRGINIA
DWIGHT EVANS, PENNSYLVANIA
BRAD SCHNEIDER, ILLINOIS
TOM SUOZZI, NEW YORK
JIMMY PANETTA, CALIFORNIA
STEPHANIE MURPHY, FLORIDA
JIMMY GOMEZ, CALIFORNIA
STEVEN HORSFORD, NEVADA

DEVIN NUNES, CALIFORNIA
VERN BUCHANAN, FLORIDA
ADRIAN SMITH, NEBRASKA
KENNY MARCHANT, TEXAS
TOM REED, NEW YORK
MIKE KELLY, PENNSYLVANIA
GEORGE HOLDING, NORTH CAROLINA
JASON SMITH, MISSOURI
TOM RICE, SOUTH CAROLINA
DAVID SCHWEIKERT, ARIZONA
JACKIE WALORSKI, INDIANA
DARIN LAHOOD, ILLINOIS
BRAD R. WENSTRUP, OHIO
JODEY ARRINGTON, TEXAS
DREW FERGUSON, GEORGIA
RON ESTES, KANSAS

GARY ANDRES,
MINORITY STAFF DIRECTOR

BRANDON CASEY,
MAJORITY STAFF DIRECTOR

May 24, 2019

The Honorable Alex M. Azar
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Secretary Azar:

I write to request detailed information regarding the Trump Administration's recent "Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties," (2019 Notice). The 2019 Notice immediately, dramatically, and without public input, reduces the total annual civil monetary penalty (CMP) applied for breaches of protected health information, sending a signal to trusted entities and criminals alike that protecting confidential medical information is not a priority.¹ In 2018, 25 percent of all cyber-attacks occurred in the health care industry.² Therefore, the Department's decision to change HIPAA enforcement standards without notice conflicts both with the reality of a vulnerable industry and the text of the statute in a way that does not preserve the American public's best interest.

The Health Information technology for Economic and Clinical Health (HITECH) Act (the Act) was intended to bolster enforcement of HIPAA violations by creating a pathway for additional resources for enforcement and oversight activities.³ Previous HHS statements have reflected a commitment to HIPAA enforcement activities; however, the 2019 Notice suggests a shift in posture.

¹ 2019 Notice, 84 Fed. Reg. 18151 (April 30, 2019). Through the 2019 Notice, the Department of Health and Human Services (HHS) adopted indefinite enforcement discretion for violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5 (February 17, 2009), incorporating the Health Information Technology for Economic and Clinical Health (HITECH) Act (the Act).

² "Managing Enterprise Risks in a Digital World: Privacy Cybersecurity, and Compliance Collide," Baker Hostetler 2019 Data Security Incident Response Report.

<http://e.bakerlaw.com/rv/ff00498db267a11ce4182d53934889997a36f6d4/p=8213342>

³ Redhead, C.S., "The Health Information Technology for Economic and Clinical Health (HITECH) Act," Congressional Research Service, April 27, 2009.

For example, press materials for the 2009 interim final rule suggested those policies were “the first of several steps HHS is taking to implement the HITECH Act’s enforcement provisions.”⁴ Similarly, the 2013 final rule sought to clarify apparently inconsistent language in HITECH while keeping with congressional intent to bolster HIPAA enforcement.⁵ Additionally, before publishing the 2019 Notice, a February 2019 HHS/Office of Civil Rights press release touted an all-time record for HIPAA enforcement penalties of \$28.7 million, up 22 percent from 2016⁶

However, the 2019 Notice immediately changed annual CMP caps while foreshadowing future efforts “to revise the penalty tiers in the current regulation to better reflect the text of the HITECH Act.”⁷ The Department made this pronouncement without presenting any indication of the timing and goals of such plans.

For almost 10 years, annual caps on CMPs for HIPAA violations have been specified in statute, yet it now appears the Administration has a different interpretation of the enforcement standards. Further, through the 2019 Notice, HHS is abdicating the policy it finalized in the rule without notice and comment rulemaking, while also noting the need to revise the current regulation to better tie to the Act. Considering the original legislative intent and recent activity in this space, I am very interested in gaining a better understanding of current HIPAA-related enforcement activities and new policies under HHS consideration.

I am concerned about HHS’s actions to implement a policy that appears at odds with statutory text and regulations. Social security numbers and health information comprise the two categories of data most at-risk for cyber-attack,⁸ and at least 30 percent of breaches reported to HHS are attributable to third-party breaches.⁹ In light of these startling realities on the vulnerability of health information alongside the Department’s push for interoperability of health information, I am not aware of any acceptable rationale for applying lesser protections for patient privacy. The continued evaluation of health technologies and introduction of new stakeholders into the health care delivery space demand continued focus on protecting Americans’ right to privacy.

⁴ “HHS Strengthens HIPAA Enforcement” U.S. Department of Health and Human Services (October 30, 2009). <https://wayback.archive-it.org/3926/20131018161347/http://www.hhs.gov/news/press/2009pres/10/20091030a.html>

⁵ 2019 Notice, 84 Fed. Reg. 18151, 18152 (April 30, 2019).

⁶ <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/2018enforcement/index.html>

⁷ 84 Fed. Reg., 18151, 18153.

⁸ “Managing Enterprise Risks in a Digital World: Privacy Cybersecurity, and Compliance Collide,” Baker Hostetler 2019 Data Security Incident Response Report.

<http://e.bakerlaw.com/rv/ff00498db267a11ce4182d53934889997a36f6d4/p=8213342>

⁹ “Third-Party Breaches in 2016 Pose Alarming Risk to Patient Data,” Breach Barometer Special Report, DataBreaches.net in collaboration with Protenus, Inc.

http://marketing.protenus.com/hubfs/Content/20160914_Databreaches.net_Full_BA_Report.pdf?hsCtaTracking=d0a07a67-ba97-49c2-b1dc-3a8410024438|427851e0-ccc7-48d6-a8c6-d4fd8e9f0688&t=1474303798162&utm_campaign=Third-Party+Breach+Report&utm_medium=email&hsen

To ensure the Committee on Ways and Means understands the status of this issue and possible need for legislative action, I respectfully ask that you respond to the following questions and requests by June 6, 2019:

1. What issues or concerns prompted HHS to revisit HIPAA enforcement at this juncture, particularly given the six-year gap since the Final Rule?
2. Which external stakeholder organizations did HHS consult with when determining how to exercise HIPAA enforcement discretion?
3. What process did HHS undertake to ensure the aggregate annual caps are sufficient for purposes of penalizing HIPAA violations and ensuring sufficient resources to continue pace with 2018's record-breaking enforcement efforts?
4. Are there any pending cases with the potential to surpass the \$16 million settlement with Anthem, Inc.? How would such cases be affected by this Notice?
5. Please provide metrics relating to HHS enforcement activities for HIPAA violations between October 30, 2009 and April 30, 2019. This should include reporting on each of the four culpability levels for (a) per-violation penalties and (b) aggregate penalties per violating person/entity for identical violations. Please designate pending matters with an asterisk and indicate the time those matters have been pending.
6. How many full-time employees have been charged with enforcement of HIPAA violations from October 1, 2009 and April 30, 2019?
7. Because the proposed interoperability policies would end HIPAA protections once data is shared with a third-party application, how will HHS ensure that violations of HIPAA are properly enforceable?

Should you have any questions, please contact Rachel Dolin of the Democratic Staff of the House Committee on Ways and Means at (202) 225-3625. Thank you for your immediate attention to this matter.

Sincerely,



Richard E. Neal
Chairman
Committee on Ways and Means